UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/724,337	11/27/2000	William F. Price, III	NA00-13402	7300

23419 7590 02/15/2005

COOLEY GODWARD, LLP
3000 EL CAMINO REAL
5 PALO ALTO SQUARE
PALO ALTO, CA 94306

EXAMINER	
JACKSON, JENISE E	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 02/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/724,337	PRICE, III, WILLIAM F.	
	Examiner	Art Unit	
	Jenise E Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-13,15-22 and 24-27* is/are rejected.

7)☒ Claim(s) *5,14 and 23* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

GB 12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

GB a)☐ All b)☐ Some * c)☒ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-2, 4, 6-8, 10-11, 13, 15-17, 19, 20, 22, 24-26, rejected under 35 U.S.C. 102(e) as being anticipated by Dyksterhouse et al.

3. As per claims 1, 10, 19, Dyksterhouse et al. discloses a method for managing public keys thorough a server that stores associations between public keys and email addresses(see col. 3, lines 29-31, col. 4, lines 13-25, et seq.); receiving a first message from a client at the server(see col. 3, lines 32-35, col. 8, lines 34-37, et seq.), the first message containing a request for approval of a client public key along with the client public key(see col. 3, lines 51-67, et seq.); sending a second message from the server to the client, the second message containing a request for identity confirmation that includes the client public key(see col. 3, lines 56-60, col. 4, lines 1-6, et seq.); and if a third message is received from the client at the server containing an affirmative response to the request for identity confirmation, storing an association between a client email address and the client public key in a database, so that other clients can look up the client public key in the database(see col. 4, lines 7-8, 13-25, et seq.).

4. As per claim 2, First, Dyksterhouse et al. discloses that the certificate server allows clients to submit and retrieve keys from a database, thus, Dyksterhouse discloses receiving a

communication from a second client at the server, the communication including the client email address(see col. 3, lines 29-31, et seq.), because Dyksterhouse discloses more than one client can make a request to the system. Further, Dyksterhouse discloses performing a lookup in the database based on the client email address to determine if the client email address is associated with the client public key, Dyksterhouse discloses this, because Dyksterhouse discloses that once a key is placed in the certificate server, clients can perform a search on the keys based on email addresses(see col. 4, lines 13-21, et seq.), if the lookup indicates that the client email address is associated with the client public key, sending a key identifier for the client public key from the server to the client, wherein the key identifier allows the client to determine whether the client possesses the client public key(see col. 4, lines 7-8, 13-25, et seq), Dykersterhouse discloses a key identifier, because Dyksterhouse discloses a key id(see col. 5, lines 26-28), each key pair has an associated key id(see col. 5, lines 26-28), thus, when the client searches for the public key by using email address, an key identifier is also associated with the public key.

5. As per claim 4, Dyksterhouse discloses decrypting the request for approval at the server using a server private key, the request for approval having been encrypted with a corresponding server public key by the client; and using the client public key to verify that the request for approval is signed by a corresponding client private key(see col. 8, lines 9-30).

6. As per claim 6, Dyksterhouse discloses receiving a request at the server to remove the client public key from the database; if the request is signed with a corresponding client private key, removing the client public key from the database(see col. 15, lines 4-12).

7. As per claim 7, Dyksterhouse discloses wherein the database contains at most one key for each email address(see col. 4, lines 13-21, et seq.).

8. As per claim 8, Dyksterhouse discloses that wherein the database contains at most one email address for each key(see col. 4, lines 13-21, et seq.).

9. As per claim 9, Dyksterhouse discloses periodically sending a verification request from the server to the client email address asking if the client public key remains valid; and if an affirmative response to the verification request is not received, removing the client public key from the database.

10. As per claim 11, it is rejected under the same basis as claim 2.

11. As per claim 13, it is rejected under the same basis as claim 4.

12. As per claim 15, it is rejected under the same basis as claim 6.

13. As per claim 16, it is rejected under the same basis as claim 7.

14. As per claim 17, it is rejected under the same basis as claim 8.

15. As per claim 20, it is rejected under the same basis as claim 2.

16. As per claim 22, it is rejected under the same basis as claim 4.

17. As per claim 24, it is rejected under the same basis as claim 6.

18. As per claim 25, it is rejected under the same basis as claim 7.

19. As per claim 26, it is rejected under the same basis as claim 8.

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. Claims 3, 12, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dyksterhouse et al. in view of Zimmermann.

22. Dyksterhouse et al. discloses a request for approval of a key(see col. 3, lines 29-35), and stores the key in the database(certificate server)(see col. 3, lines 35-40). However, Dyksterhouse does not disclose key reconstitution information. However, Zimmermann discloses key reconstitution information(i.e. message recovery key), that allows the client to decrypt to an encrypted client private key at the client(see col. 3, lines 30-40) if the client forgets a passphrase for decrypting the encrypted client private key, and storing the key reconstitution information in the database(see col. 3, lines 1-10).

23. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Dyksterhouse with Zimmermann to have key reconstitution information that when a user forgets a passphrase a user can decrypt with a key, the motivation to include key reconstitution information in Dyksterhouse, is that oftentimes there exists a need for an authorized party other than the sender of a recipient to have access to an encrypted message since the recipient of the message might not always be available(see col. 2, lines 60-64). Dyksterhouse recognizes this problem and gives an examples of which the recipient may not be available: for instance the employee has left the company or is away on vacation, or another scenario, the employee is available but he or she has lost his or her private key, which is needed to decrypt the encrypted e-mail message(see col. 3, lines 2-5 of Zimmermann). Dyksterhouse also recognizes that if the key is lost, that this occurs if the user forgets the passphrase that is required to access his or her private key(see col. 3, lines 5-8 of Zimmermann). Thus, including key reconstitution of Zimmermann with Dyksterhouse, enables one to decrypt an encrypted message so that

authorized parties other than the recipient can access to the encrypted message(see col. 3, lines 7-10).

24. Claims 9, 18, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dyksterhouse(6336186) et al. in view of Zubeldia et al(6044462).

25. Dyksterhouse et al. discloses a client that request a server to allow the client to retrieve keys from the server(see col. 3, lines 29-34). The keys are associated with an e-mail address(see col. 4, lines 13-21). However, Dyksterhouse does not disclose asking if the client public key remain valid; and removing the client public key from the database. Zubeldia et al. discloses asking if the client public key remain valid; and removing the client public key from the database(see col. 3, lines 21-26).

26. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Dyksterhouse with Zubeldia et al. to include asking if the client public key remains valid and removing the client public key from the database, the motivation is that a certificate remains valid unit the operational life of the certificate has expired(see col. 2, lines 62-67 of Zubeldia et al.), if the certificate is not valid it has been revoked(see col. 3, lines 1-4 of Zubeldia et al), and when the certificate is no longer valid it is removed from the database, because the certificate could have been revoked due to the certificate being compromised(see col. 3, lines 60-67 of Zubeldia).

27. Claims 5, 14, and 23 are object to as being rejected on base claims. The reasons why these claims are allowable are, if the database already contains the prior client public key, including the prior client public key in the request so that the server can replace the prior client public key with the client public key. In prior art of digital certificates, the client does not

request the server to replace the prior client public key with the client public key, the server or ca has a certificate stored in the database that has a validity period associated with it, and when the validity period is about to expire or has expired, the old certificate is replace with a new certificate in prior art this replacement is done automatically, the client does not request this to happen.

Response to Amendment

28. The Applicant states that the server does not communicate with the client. The Examiner disagrees with the Applicant. Dyksterhouse et al. discloses the certificate server of Dykersterhouse, allows the clients to submit keys to a database(see col. 3, lines 32-35, col. 8, lines 31-36). This submitting of keys by Dykersterhouse is the request.

29. The Applicant states that sending a second message from the server to the client, the second message containing a request for identity confirmation that includes the client public key. The Examiner disagrees with the Applicant. The server accepts requests from certificates of a client, the identity confirmation of the user is the access level of the user(see col. 3, lines 56-61). The policy agent of the server checks to see if the identity confirmation of the user corresponds with the certificate of the user(see col. 3, lines 59-67, col. 4, lines 1-6).

30. The Applicant states that a third message is not disclosed in Dyksterhouse. The Examiner disagrees with the Applicant. The third message of Dyksterhouse is that a key is placed on the PGP server and thus it can be retrieved by the client. Once this key is placed on the PGP server, it is a message to the client, that the keys can be access by the LDAP search retrieval functions(see col. 4, lines 13-21) The keys can be searched by certain attributes, such as an e-mail address(see col. 4, lines 18-21).

Final Action

31. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

February 7, 2005